Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

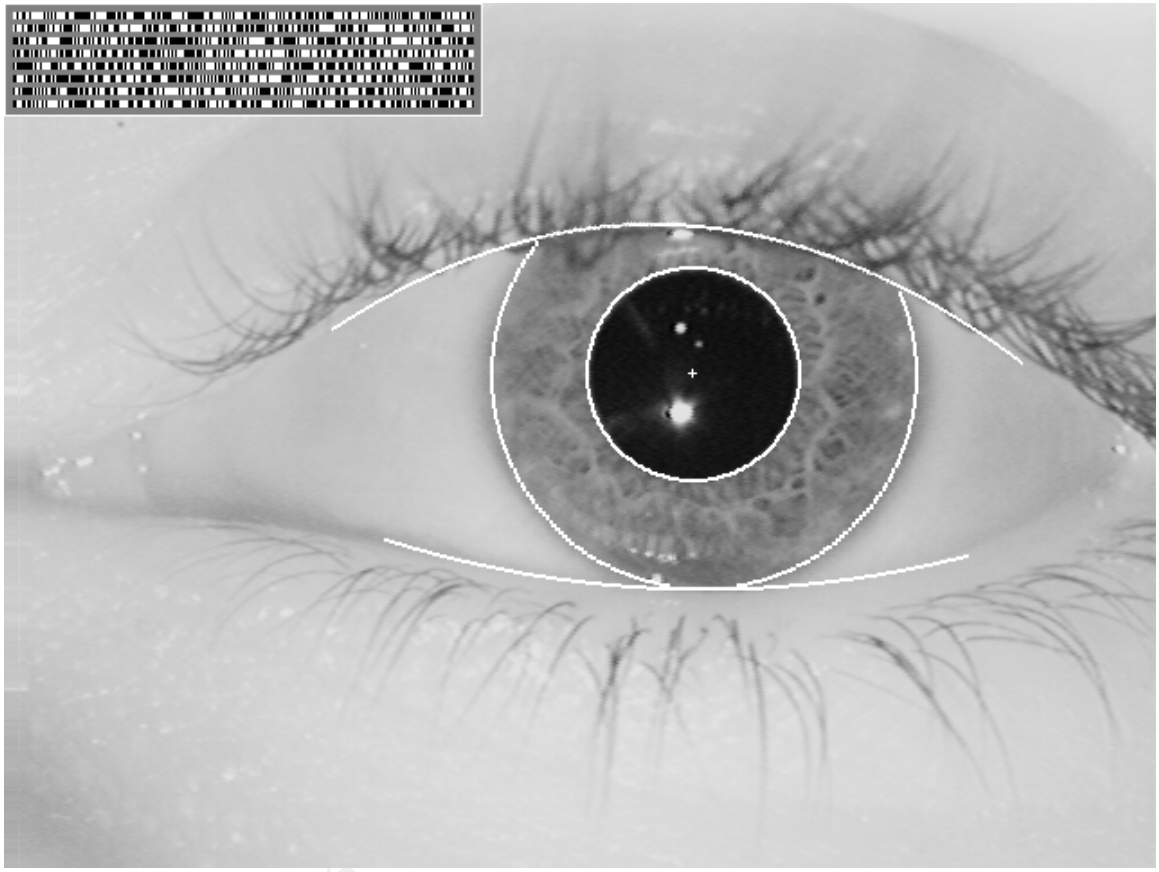
Dont Blink:Iris Recognition for Biometric Identification

With the cost of eye-scanning technology coming down and the need for more secure systems going up, it's time to take a close look at iris recognition for security applications. Due to research and patented technology, iris recognition has emerged from its early image of spy film fantasy to reality. This paper explores the origins of iris recognition, how it works, how it stacks up against other forms of biometric identification and what is required to perform the identification. Comparisons will be made to fingerprint...

Copyright SANS Institute
Author Retains Full Rights

AD

Don’t Blink: Iris Recognition for Biometric Identification



Eye and IrisCode [1]

Mary Dunker
SANS Security Essentials, July 2003
GSEC Certification Practical, Version 1.4b
Submitted November 20, 2003

[1] Daugman, John. Home page. 18 November 2003.
<http://www.cl.cam.ac.uk/users/jgd1000/iriscode.gif>

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Don't Blink: Iris Recognition for Biometric Identification

Summary

With the cost of eye-scanning technology coming down and the need for more secure systems going up, it's time to take a close look at iris recognition for security applications. Due to research and patented technology, iris recognition has emerged from its early image of spy film fantasy to reality. This paper explores the origins of iris recognition, how it works, how it stacks up against other forms of biometric identification and what is required to perform the identification. Comparisons will be made to fingerprinting, retinal scanning, speaker recognition, facial scanning and hand geometry.

We will report on products that are on the market today to help implement iris recognition technology and will examine some existing and proposed real-world applications that take advantage of iris recognition for secure biometric identification and authentication. The information and conclusions drawn in this paper should help others who are investigating the usefulness of iris recognition for secure biometric identification.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Origins

In 1936, ophthalmologist Frank Burch conceived the idea of using the iris for identification.[2] Many of us remember seeing the eye-scanner used in James Bond films, but it took almost 60 years for the technology to become reality. Ophthalmologists Aran Safir and Leonard Flom patented the idea of using the iris for identification in 1987. In 1989, they enlisted the help of Harvard Professor John Daugman to develop iris recognition algorithms, which he subsequently patented. Safir, Flom and Daugman formed a partnership, and the algorithms are now owned by Iridian Technologies.[3]

John Daugman is currently a Professor at Cambridge University, where he has received numerous awards for his work on iris recognition algorithms. The awards include the British Computer Society's IT Award and Medal in 1997, the Smithsonian Award in 2000, the "Time 100" Innovator Award in 2001, and the Millennium Product designation by the UK Design Council in 1998.[4]

John Daugman: His Research

Although other research exists in the iris recognition field, the work done by John Daugman is prominent in that it has produced commercial products and applications that implement iris recognition technology. In 1993, John Daugman wrote his original scientific paper called "High confidence visual recognition of persons by a test of statistical independence." This is published in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15(11), pp. 1148-1161.[5] He developed a computerized process to generate a binary encoded template called an IrisCode® from a camera image taken of an iris. His algorithms are then used to compare IrisCodes for identity verification. Daugman maintains a web site at http://www.cl.cam.ac.uk/jgd1000 that includes reference papers that describe his algorithms and iris recognition technology.[6]

Iridian Technologies holds exclusive rights to the algorithms of John Daugman, and Iridian licenses the algorithms to system integrators and developers. Initiatives in iris recognition applications have been explored or implemented by

---

[2] Mrozek, Werner. "IriScan – Biometrics for secure recognition." December 2000. Biometric News. 7 November 2003. <http://www.euro-security.de/en/html/iriscan_-_biometrics_for_secur.html>.

[3] Daugman, John. "History and Development of iris Recognition." Daugman, John. Home page. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/history.html>.

[4] Daugman. "History."

[5] Daugman, John. "High confidence visual recognition of persons by a test of statistical independence." 11 November 1993. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15(11), pp. 1148-1161. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/PAMI93.pdf>.

[6] Daugman, John. "Iris Recognition for Personal Identification." Daugman, John. Home page. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/iris_recognition.html>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

partnerships between Iridian and Diebold, Panasonic, LG, EyeTicket Corporation IBM, NCR and Oki[7]. Some of these companies' products and services will be described in more detail later in this paper.

Technical Description

Physiology

The iris is the colored part of the eye that lies behind the cornea, in front of the lens, and is protected by the eyelid. John Daugman points out that the iris is the only internal organ of the human body that is normally externally visible. The iris is formed of a trabecular meshwork (elastic connective tissue), layers of pigment, muscle and ligaments, and it controls the amount of light that enters the eye by allowing the pupil to dilate. Color is not used in iris recognition technology. Instead, the other visible features such as the connective tissue, cilia, contraction furrows, crypts, rings and corona distinguish one iris from another.[8]

By the time a human is about eight months old, the iris' structures are complete, and they do not change in later life. The iris cannot be surgically altered without damage to a person's vision, and its physical response to light provides one test that prevents artificial duplication of the organ.[9] As with a fingerprint, the iris has a random structure of minutiae or points of detail that can be encoded to form a distinctive template. No two irises are alike, even if they are from identical twins or the left and right eye in the same person.[10] Its physiological characteristics combined with the fact that those characteristics are exhibited with so much variation over the population, make the iris a prime candidate for use in identity verification.

Encoding

As John Daugman describes in "How Iris Recognition Works," the iris contains complex patterns of ligaments, furrows, ridges, crypts, rings and corona that allow algorithms to be produced that can be used to identify an individual. By using a pseudo polar coordinate system, iris images can be represented that do not vary with factors such as the distance from the eye to the camera, the size of the pupil, the location of the iris within the image or the angle and orientation of the iris image due to different camera angles.[11]

---

[7] Daugman. "History."
[8] Daugman, John. "Anatomy and Physiology of the Iris." Daugman, John. Home page. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/anatomy.html>.
[9] Daugman, "Anatomy".
[10] Daugman, "Anatomy".
[11] Daugman, John, "How Iris Recognition Works.", p. 6. Daugman, John. Home page. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf >.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

An IrisCode is created by encoding the variable structures of the iris. Using a camera to record the image, the inner and outer boundaries of the iris are first determined, taking into account the contours of the eyelid and discounting eyelashes, reflections and contact lens boundaries. The patterns are then encoded using 2D Gabor wavelet demodulation to create a phase code that is similar to a DNA sequence code. 2048 bits of data plus 2048 masking bits are used to produce a 512-byte IrisCode.[12] About 250 degrees of freedom or independent dimensions of variability are represented in the IrisCode.[13] In order to enroll a person for future identification, the IrisCode is stored in a database or on a smart token.

Verification and Identification

Iris recognition technology can be used for both positive and negative identification. Positive identification (verification) confirms that a person is who he or she claims to be. Negative identification compares features of one person to those of many to prove that a person is not who he or she says she is not. We will refer to positive identification as verification and negative identification as identification because this is how the terms were used in the studies we cite.

Daugman's iris recognition process for verification and identification involves comparing IrisCodes by performing Boolean XOR operations and computing a function called the Hamming Distance, as a measure of dissimilarity between any two irises. In a test for statistical independence, the test will be passed when IrisCodes for two different eyes are compared, and the test will fail when two IrisCodes for the same eye are compared. Thus, "The key to iris recognition is the failure of the test for statistical independence."[14]

The Hamming Distance can be computed with extreme speed because of the way computers handle Boolean operations and the fact that the operations can be performed in parallel. It would only take 1.7 seconds to compare one million IrisCodes on a 2.2GHz computer.[15] This level of performance makes iris recognition technology feasible for very large-scale applications where millions of IrisCodes can be compared using multiprocessing techniques.

Biometric identification processes employ decision-making thresholds that must select trade-offs between the False Accept Rate (FAR) and the False Reject Rate (FRR). Using Daugman's Hamming distance calculation, the probability of getting a False Accept when two irises match in more than 75% of their IrisCode

---

[12] Daugman, "How Iris Recognition Works."
[13] Daugman, John. "Demodulation by Complex-Valued Wavelets for Stochastic Pattern Recognition." 18 November 2002. International Journal of Wavelets, Multiresolution and Information Processing Vol.1 No.1. (2003): 1-17.
[14] Daugman, John. "Iris Matching Engine, and Search Speed." Daugman, John. Home page. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/search.html>.
[15] Daugman. "Iris Matching."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

bits is only one in 10 raised to the 14th power. This extremely low probability of getting a false match allows the iris recognition algorithms to be used on extremely large databases without error.[16] Daugman has shown that the probability of more than two-thirds of the bits of two IrisCodes from different eyes matching just by chance is mathematically extremely low.[17] This makes iris recognition a very reliable form of biometric identification.

Implementing the Technology

What does it take to implement iris recognition? Start with a video camera, a computer and some software. Iridian describes the steps involved in iris recognition as follows.[18]

Imaging

First, an image must be captured by a camera. A Charge Coupled Device (CCD) camera is used and must be compliant with ANSI/IESNA RP-27.1-96 and IEC 60825-1 standards for radiation and laser products. The subject is 5 inches to 2 feet away from the camera and looks at a LED guide to ensure that the camera focuses on the iris.

IrisCode Creation and Enrollment

After the image is captured on camera, an IrisCode is created as described earlier in the "Technical Description." To enroll a person, the IrisCode is stored in a database or on a smart token. IrisCodes are created using the same process for initial enrollment and for verification or identification, but only the enrollment phase requires storing the IrisCode.

Recognition

In order to verify that a person is who he or she claims to be, a camera image is taken again, a new IrisCode is generated, and a comparison is made between the IrisCode just created and a single IrisCode on a smart token or in a database. For identification purposes, the newly created IrisCode is compared to all existing IrisCodes in a database. In both cases, the recognition phase includes the Hamming Distance calculation and the XOR comparison described in the "Technical Description" section of this paper. Typically, the Boolean comparison is made in a matter of seconds. A match (failure of statistical independence test) proves that the person is the same one whose iris was enrolled at an earlier time.

---

[16] Daugman, John. "Decision environment for iris recognition." Daugman, John. 7November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/decidability.html>.

[17] Daugman, John. "Binomial Distribution of IrisCode Hamming Distances." Daugman, John. 7 November 2003. http://www.cl.cam.ac.uk/users/jgd1000/binomdata.html.

[18] Iridian Technologies. Home page. 7 November 2003. http://www.iridiantech.com/how/index.php?page=3.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Iris Recognition versus Other Biometric Technologies

Three factors can be used for security: something you know (password or PIN), something you have (smart token or access card), and something you are (biometric). Biometrics can be used alone or in conjunction with one of the other factors to strengthen the security check. Biometric technology has advantages over both of the other factors in that the user does not need to remember anything or possess a physical token in order to be identified. Tokens and cards can be lost, and passwords and PINs can be forgotten or compromised. A biometric is only susceptible to forgery, which can be extremely difficult, depending on the biometric.

Iris recognition falls into the physical biometric category as opposed to behavioral biometrics such as signatures.[19] Other physical biometric technologies include fingerprinting, retinal scanning, speaker recognition, facial scanning and hand geometry. The National Center for State Courts (NCSC) published information comparing these physical biometric methods.[20] The NCSC data is substantiated by a similar comparison table found at the IEEE Computer Society.[21] Here are some highlights from both groups' findings.

Fingerprinting

Iris recognition shares many characteristics with fingerprinting. Both biometric technologies are reliable and very accurate, but iris recognition has a much lower error rate (1 in 131,000) than fingerprinting (1 in 500+).[22] (The NCSC defines error rate as the crossing point of the graphs of false positives and false negatives of a particular biometric.) Both biometric methods can be used to verify that a person is who he or she claims to be and to identify a person by comparing the current biometric input to a large set of data that was previously recorded. According to the NCSC, false positives and false negatives are difficult to produce for both fingerprinting and iris recognition.[23] False acceptance rates are extremely low for iris recognition. Tests conducted through December 2000 had not resulted in a single false acceptance of an iris.[24] Both fingerprints and iris are stable physical characteristics that do not change with age.

---

[19] Penny, Wayne. "Biometrics: A Double Edged Sword – Security and Privacy". 2003. SANS Reading Room. 7 November 2003. <http://www.sans.org/rr/papers/index.php?id=137>.
[20] "Biometrics Comparison Chart". 2002. NCSC Court Technology Lab. 7 November 2003. <http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html>.
[21] "A Practical Guide to Biometric Security Technology". 2001 IT Professional: Technology Solutions for the Enterprise. 7 November 2003. <http://www.computer.org/itpro/homepage/jan_feb01/security3b.htm>.
[22] "Biometrics Comparison Chart."
[23] "Biometrics Comparison Chart."
[24] Mrozek, Werner.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

However, since older people tend to have drier skin, fingerprints can be more difficult to verify as a person ages.

Fingerprinting hardware is generally less expensive than that for iris recognition, but recent technology is lowering costs of iris recognition devices.[25] External factors can cause errors in both fingerprinting and iris recognition. Fingerprints can be affected by dirt, dryness and scarring. Iris recognition can be affected by lighting. Both technologies are reasonably well accepted by the user population, but fingerprinting was rated more intrusive than iris scanning.[26] This rating may be due to the requirement to make physical contact with a fingerprinting device. Fingerprinting may also carry some negative connotations due to its historical use in criminal investigations.

There are some health related advantages of iris recognition over fingerprinting. Fingerprinting requires physically touching a device each time the finger is presented for verification. In contrast, the iris template is created without any physical contact with the person whose iris is encoded. The iris recognition process is, therefore, more appealing to those concerned with hygiene than is fingerprinting.

Forgery is not as much of a risk with iris recognition as with fingerprinting. Although sophisticated fingerprinting technology is designed to detect false fingers, a person's finger can be cut off or used for a mold much easier than an eyeball could be extracted and used for impersonation. In fact, the iris from a person's extracted eye would not be usable for more than a few seconds.[27] Iris recognition devices can also detect the dilating pupil to ensure that the eye is live.

Retinal Scanning

Retinal scanning is often confused with iris recognition, but they are very different biometric technologies. The retina is located at the back of the eye and contains distinctive vascular patterns that can be used for identification and verification. Retinal scanning is the only biometric that is more reliable than iris recognition. The error rate for retinal scanning is 1:10,000,000 compared to the iris recognition error rate of 1:131,000. [28] The retinal scanning process is different from iris recognition and does not involve an IrisCode. Both retinal and iris technologies are extremely accurate and reliable and have very low false acceptance rates.

---

[25] "Interactive Buyer's Guide: Biometric Authentication." 2003. Network Computing. 7 November 2003..
http://ibg.networkcomputing.com/ibg/Chart?guide_id=4164.
[26] "Biometrics Comparison Chart."
[27] Soto, Carlos A.. "Biometrics gets better but still needs some work". Government Computer News 05/05/03; Vol 22 No. 10. 7 November 2003.
<http://www.gcn.com/22_10/prod_reviews/21949-1.html>.
[28] "Biometrics Comparison Chart."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Opinions seem to differ on which feature, iris or retina, is more reliable to use throughout life. According to John Marshall of Retinal Technologies, "The iris is harder to map as an image because it fluctuates based on the size of the pupil, and drug or medicinal use, and age. The retina stays constant throughout your life, unless you have glaucoma or diabetes."[29] True, the iris is not fully shaped until about eight months of age, but after that age, it is commonly believed to be stable.

As depicted in the movie, "Minority Report," retinal scanning is a much more intrusive process than iris recognition. A retinal scanning subject must stay very still, with the eye at a distance of no more than 3 inches from the scanner, whereas iris recognition can be accomplished with the subject at a distance of up to about 2 feet from the camera. People wearing glasses must remove them for a retinal scan. For iris recognition, the National Physical Laboratory (NPL) tests found that glasses can make enrollment more difficult, but they can remain in place for verification without causing difficulty.[30] The NPL tests revealed difficulty in enrolling a blind person's iris because the system required both eyes to be enrolled.[31] Depending upon the nature of the blindness, enrollment of two eyes using retinal scanning might also be prohibitive. No NPL data was reported for retinal scans of blind eyes.

Neither technology has been inexpensive in the past, but recent developments are bringing prices down for both iris recognition and retinal scanning. Retinal scans are probably most appropriate for applications that require the highest levels of security, where the subject is very cooperative and patient, or is required by law to succumb to the scan.

Speaker Recognition

Of the physical biometric technologies discussed in the NCSC comparison, speaker recognition ranks highest in user acceptance, and is easier to use and less expensive than iris recognition. With an error rate of 1 in 50, speaker recognition is much less accurate than iris recognition.[32] False negatives are easy to produce, and the errors can occur due to noise and colds. Speaker recognition could be used to verify a person's identity, comparing to a previously stored template for a person, but is not recommended for identification. Iris recognition is recommended for both verification and identification.[33]

---

[29] French, Matthew. "Retinal eyes biometric security". . Aug 6-12, 2001. Mass High Tech: The Journal of New England Technology, vol. 19, issue 32. 7 November 2003. http://www.retinaltech.com/retinal.pdf.

[30] Mansfield, Tony, Gavin Kelly, David Chandler, and Jane Kane. CESG Contract X92A/4009309 Biometric Product Testing Final Report.. Draft 0.6. Middlesex: National Physical Laboratory, 19 March 2001.

[31] Mansfield

[32] "Biometrics Comparison Chart."

[33] "Biometrics Comparison Chart."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Facial Recognition

Similar to iris recognition, facial recognition requires a subject to present his or her face to a camera. Both technologies are non-intrusive, but they differ in that the subjects in facial recognition need not know their identity is being captured on camera. This aspect can be beneficial in areas where it is important to confirm identity without the subject's knowledge, but the anonymity with which a facial image can be captured also raises a privacy issue that is not present with iris recognition. Iris recognition is more reliable than facial recognition.[34] The NPL study cites a false accept rate of 1:100 for facial recognition versus 1:1.2 million for iris recognition.[35]

Hand Geometry

The NCSC chart lists hand geometry as one of the easier to use biometric technologies, but it is not as accurate as either iris recognition or retinal scanning. The error rate for hand geometry is 1 in 500 compared to 1 in 131,000 for iris recognition.[36] Another drawback of hand geometry technology is that it is relatively easy to produce a false negative, since hand features are not distinctive.[37] Therefore, the technology is not well suited for identification. It should work well enough for verification as long as the device can recognize a fake hand. Unlike the iris, hand characteristics could change over time due to scars and growth patterns. Hand geometry has the same hygiene issue as fingerprinting.

Market Resources

Software and hardware systems are available today that assist in implementing iris recognition. Iridian's PrivateID®, Iris Authentication Agent for Computer Associates *e*Trust Single SignOn 1.0, Iris Authentication Agent for Netegrity Siteminder v1.0, SecureSuite 3.1 and SecureSuite 2.3. are all based on Iridian's iris recognition technology.[38] The review done by Government Computer News utilized the Saf2000 tool from SafLink Corporation to conduct its test of biometric products that included the Panasonic Authenticam™ that uses PrivateID.[39]

---

[34] "Biometrics Comparison Chart."
[35] Mansfield.
[36] "Biometrics Comparison Chart."
[37] "Individual Biometrics – Hand Geometry." 2002. NCSC Court Technology Lab. 7 November 2003.
"http://ctl.ncsc.dni.us/biomet%20web/BMHand.html".
[38] "Proof Positive: Certification Configuration." 2003. Iridian technologies: Proof Positive. 7 November 2003.
http://www.iridiantech.com/products.php?page=5&sub=a.
[39] Soto. Carlos A. "Biometrics gets better but still needs some work." Government Computer News Vol. 22 No. 10. May 2003. 7 November 2003.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Several companies are manufacturing cameras that work in conjunction with the Iridian technology for iris recognition. The cameras are used with PrivateID and KnoWho® software from Iridian.

Panasonic offers multiple cameras.[40] The compact BM-ET300 mounts on the wall and can enroll two irises at once. The BM-ET100US (Authenticam™) is designed for use with a PC for secure biometric access in less than 2 seconds. In May 2003, GCN declared the Authenticam™ as Reviewer's Choice when combined with Iridian's PrivateID and KnoWho software.[41] This camera can also be used for Windows videoconferencing. The BM-ET500 monitors access and entry status and is ideal for offices, factories and airports.

Detailed descriptions of the Panasonic iris recognition products can be found at http://www.panasonic.com/security.

LG Electronics manufactures the LG IrisAccess 3000 for Windows users and ICU3000 for Linux platforms. IrisAccess is an easy-to-use one-eye auto-focus camera that operates at a distance of 3 to 10 inches from the iris. The ICU3000 is a server-based product.[42]

OKI markets IrisPass® with two choices in products. The WG line is a gate control system, appropriate for vaults, data centers, storage facilities and other areas where physical access must be controlled. IrisPass-h is used with handheld devices to control computer login access for Windows.[43]

Practical Applications

Iris recognition systems are being used today to control physical access, to facilitate identity verification and for computer authentication. Real-world iris recognition applications have been implemented for airport and prison security, automatic teller machines, authentication using single sign-on, to replace ID cards, and to secure schools and hospitals.[44]

<http://www.gcn.com/22_10/prod_reviews/21949-1.html>.

[40] "Product Showcase." 2003. Panasonic Ideas for Life.7 November 2003. <http://www.panasonic.com/cctv/showcase/>.

[41] Soto.

[42] "LG Iris Recognition System – IrisAccess 3000." 2003. LG Electronics / Iris Technology Division. 7 November 2003. <http://www.lgiris.com>.

[43] "IrisPass." 2001-2002. OKI Global Site. 7 November 2003. <http://www.oki.com/jp/FSC/iris/en>.

[44] "Selected Solutions: Selected Case Studies." 2003. Iridian Technologies. 19 November 2003. http://www.iridiantech.com/solutions.php?page=2.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Airport Security

One of the most promising applications for iris recognition increases security for the transportation industry. In 2000, the Charlotte/Douglass Airport in Charlotte, NC and Flughafen Frankfurt Airport in Germany began tests to register and identify passengers using the EyePass™ system from EyeTicket. In Charlotte, US Airways flight staff were also enrolled.[45] In June of 2001, Congress requested $2.75 million to expand the program at Charlotte/Douglas International. At the time of the request, over 300,000 iris recognitions had been performed with 100% accuracy and no security breaches. [46] EyePass™ continued to perform well and was fully functional at Charlotte/Douglas by April of 2003. [47] EyeTicket also offers a completely automatic passenger service called JetStream™ that has been installed at London's Heathrow Airport.[48]

In April 2002, in a partnership with Schiphol Group of Amsterdam, IBM made plans to offer an airport security access system using iris recognition. The IBM system is based on an Automatic Border Passage system that Schiphol Group deployed at Amsterdam Airport Schiphol.[49] The system is designed to be used by passengers and by airport staff for secure access to restricted airport areas. At the Schiphol airport, smart cards are used to record the passenger's iris template and then verify their identity at the gate. The Border Passage system uses the LG2200 camera. The verification procedure substitutes for the standard manual passport check and takes 10-15 seconds.

New York's JFK, Washington's Dulles and 14 international airports in Canada have either tested or installed an iris recognition system.[50]

ATM

Someday, it may be common for ATM users to be identified by their irises rather than their PIN numbers. Bank United Corporation in Houston, Texas began

---

[45] Meehan, Michael. "Iris scans take off at airports." July 2000. ComputerWorld. 7 November 2003.
<http://www.computerworld.com/securitytopics/security/story/0,10801,47202,00.html >.

[46] "Congress Requests 2.75 Million to Expand Iris Recognition at Charlotte/Douglas International Airport." 13 June 2001. EyeTicket Press Releases. 8 November 2003.
<http://www.eyeticket.com/en/releases2001.php?date=06132001.htm&about=none>.

[47] "EyeTicket, Charlotte/Douglas Airport Set New Standard in Security Access Control with Launch of Precedent-setting EyePass." 13 April 2003. EyeTicket Press Releases. 8 November 2003.
http://www.eyeticket.com/en/releases.php?date=04162003.htm&contact=ckali&about=none.

[48] "Jetstream." 1999-2002. EyeTicket Products. 8 November 2003.
http://www.eyeticket.com/en/index.php?section=products&body=jetstream.

[49] "IBM Looks Airline Security in the Eye." 25 April 2002. IBM News. 8 November 2003.
< http://www-1.ibm.com/industries/wireless/doc/content/news/pressrelease/291888104.html>.

[50] Henahan, Sean. "The Eyes Have It." 6/17/2002. Access Excellence: Science News: Iris Scan – Eye on Security. 8 November 2003.
http://www.accessexcellence.org/WN/SU/SU102001/irisscan.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

using iris recognition at its Automatic Teller Machines in supermarkets in May of 1999. [51] In 1998, Nationwide Building Society, a bank in Swindon, Wiltshire, introduced iris recognition to replace PIN numbers in ATMs.[52] The system being tested by Nationwide would allow a person's IrisCode to be stored either in a central database or on a card.[53] The ability to store the IrisCode on a smart card or token is important because it eliminates privacy concerns associated with retaining identities in a centralized database.

Authentication and Single Sign-on

A biometric technology such as iris recognition can easily eliminate or complement the standard login password for individual authentication to a computer. Providing multi-factor authentication is one of the great benefits of biometric technology. Iris recognition for Windows authentication is provided with PrivateID and KnoWho software packages. The ability to support single sign-on goes a step further to enable biometric authentication to be integrated into enterprise class applications. Iridian supports an implementation of single sign-on with Computer Associates™ *e*Trust Single Sign-on, which works in conjunction with Iridian's PrivateID and KnoWho Authentication Server. PrivateID is used with a camera device to capture the iris image. KnoWho generates an IrisCode and compares it with IrisCodes stored in either an SQL or Oracle database, depending on the server platform. CA's *e*Trust Single Sign-on client allows iris recognition plug-in modules to effect authentication. The *e*Trust server provides the central repository for storing credentials.[54]

Replacing ID Cards for Students

In Ryhope, England, the Venerable Bede School uses iris recognition in lieu of ID cards for its students.[55] In the fall of 2003, the school implemented Impact from the Scottish company CRB Solutions. The Impact system integrates an iris recognition camera into a cashless catering system so that students are identified, and their meals are automatically charged to an account. The cashless system puts all students on equal financial ground by not revealing which students are receiving subsidized meals. The iris recognition devices are also employed to allow students to borrow library books and to restrict access to certain areas in the school.

---

[51] Meehan.
[52] Henahan.
[53] Hawkes, Nigel. "Machines will pay up in blink of an eye." Daugman, John. Home page. 8 November 2003.
http://www.cl.cam.ac.uk/users/jgd1000/atm.jpg
[54] "Integrating Computer Associates' eTrust Single Sign-on with Iris Recognition Technology." Iridian™ Technologies.
[55] Akumanyi, Kofi. "Eye-Opening Way to Get Lunch." British Embassy Berlin. 15 November 2003. < http://www.britischebotschaft.de/en/embassy/r&t/notes/rt-news030926_get_lunch.htm>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Conclusions

Based on the applications, reliability, ease of use, and software and hardware devices that currently support it, iris recognition technology has potential for widespread use. Iris recognition costs compare favorably with many other biometric products on the market today.[56] Next to retinal scanning, iris recognition is the most secure biometric technology available. Iris recognition removes the need for physical contact with the biometric recording device and is recommended for both verification and identification. The algorithms developed for iris recognition have been well tested and perform well when implemented on today's computer hardware.

So why are there not iris recognition devices in every airport, at every bank's ATM and at every server and workstation? For computer login, cost and portability may be factors. Even though a camera and software can be purchased today for $239.00,[57] the costs add up when a device must be added to each workstation. The cameras, while small, are still more bulky than a workstation fingerprint reader and would probably be cumbersome to carry around to facilitate logging in to a laptop. On the other hand, the ability to use an iris recognition camera as a video conferencing device may make up for the camera's bulk, and makes iris recognition a more attractive biometric authentication choice for standard desktop configurations.

For ATMs at banks, iris recognition seems to be the perfect biometric. However, it will take longer to enroll customers using a biometric device than it does to simply assign and change a PIN. Since cards with PINs are already in use, it may be a while before any type of biometric device becomes prevalent in the banking industry. The beauty of iris recognition, however, is that it is non-intrusive and very secure, and it could eliminate the need for a card for ATM transactions. This could drastically reduce the effects of credit card theft because the cards would be useless at the ATM. Secure banking that relies on who you are rather than what you have would certainly be convenient.

The increase in requirements for securing airports could drive up the use of biometric devices for transportation security. Since there were not many identification/verification systems in airports prior to September 11, 2001, the opportunity is ripe to install state-of-the-art identification systems for travelers. Iris recognition systems seem to fill that need well, and there is already evidence that the transportation industry recognizes the usefulness of iris recognition. Terrorist activity increases the need for secure access to restricted areas, so there may also be increases in installation of biometric devices for building entry. In addition to its reliability, the lack of physical contact required for verification

---

[56] "Interactive Buyer's Guide: Biometric Authentication." 2003. Network Computing. 8 November 2003. http://ibg.networkcomputing.com/ibg/Chart?guide_id=4164>.

[57] "Interactive Buyer's Guide."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

may make iris recognition more attractive to the general public than fingerprint or hand geometry biometric devices.

Iris recognition has made great strides in the last 5 years. It scores well compared to the other biometric technologies, both in ease of use and in reliability. Perhaps someday, iris recognition will be prevalent for many more applications, and the only thing the user will need to remember is, “Don’t blink!”

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

Akumanyi, Kofi. "Eye-Opening Way to Get Lunch." British Embassy Berlin. 15 November 2003. < http://www.britischebotschaft.de/en/embassy/r&t/notes/rt-news030926_get_lunch.htm>.

"Biometrics Comparison Chart". 2002. NCSC Court Technology Lab. 7 November 2003.<http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html>.

"Congress Requests 2.75 Million to Expand Iris Recognition at Charlotte/Douglas International Airport." 13 June 2001. EyeTicket Press Releases. 8 November 2003. <http://www.eyeticket.com/en/releases2001.php?date=06132001.htm&about=none.>

Daugman, John. "Anatomy and Physiology of the Iris." Daugman, John. Home page. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/anatomy.html>.

Daugman, John. "Binomial Distribution of IrisCode Hamming Distances." Daugman, John. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/binomdata.html>.

Daugman, John. "Decision environment for iris recognition." Daugman, John. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/decidability.html>.

Daugman, John. "Demodulation by Complex-Valued Wavelets for Stochastic Pattern Recognition." 18 November 2002. International Journal of Wavelets, Multiresolution and Information Processing Vol.1 No.1. (2003): 1-17.

Daugman, John. "High confidence visual recognition of persons by a test of statistical independence." 11 November 1993. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15(11), pp. 1148-1161. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/PAMI93.pdf>.

Daugman, John. "History and Development of iris Recognition." Daugman, John. Home page. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/history.html>.

Daugman, John. Home page. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/iriscode.gif>.

Daugman, John, "How Iris Recognition Works." p. 6. Daugman, John. Home page. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf >.

Daugman, John. "Iris Matching Engine and Search Speed." Daugman, John. Home page. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/search.html>.

Daugman, John. "Iris Recognition for Personal Identification." Daugman, John. Home page. 7 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/iris_recognition.html>.

"EyeTicket, Charlotte/Douglas Airport Set New Standard in Security Access Control with Launch of Precedent-setting EyePass." 13 April 2003. EyeTicket Press Releases. 8 November 2003. <http://www.eyeticket.com/en/releases.php?date=04162003.htm&contact=ckali&about=none>.

French, Matthew. "Retinal eyes biometric security". . Aug 6-12, 2001. Mass High Tech: The Journal of New England Technology, vol. 19, issue 32. 7 November 2003. <http://www.retinaltech.com/retinal.pdf>.

Hawkes, Nigel. "Machines will pay up in blink of an eye." Daugman, John. Home page. 8 November 2003. <http://www.cl.cam.ac.uk/users/jgd1000/atm.jpg>.

Henahan, Sean. "The Eyes Have It." 6/17/2002. Access Excellence: Science News: Iris Scan – Eye on Security. 8 November 2003. <http://www.accessexcellence.org/WN/SU/SU102001/irisscan.html>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

"IBM Looks Airline Security in the Eye." 25 April 2002. IBM News. 8 November 2003. < http://www-1.ibm.com/industries/wireless/doc/content/news/pressrelease/291888104.html>.

"Individual Biometrics – Hand Geometry." 2002. NCSC Court Technology Lab. 7 November 2003. "http://ctl.ncsc.dni.us/biomet%20web/BMHand.html".

"Integrating Computer Associates' eTrust Single Sign-on with Iris Recognition Technology." Iridian™ Technologies.

"Interactive Buyer's Guide: Biometric Authentication." 2003. Network Computing. 7 November 2003. <http://ibg.networkcomputing.com/ibg/Chart?guide_id=4164>.

Iridian Technologies. Home page. 7 November 2003. <http://www.iridiantech.com/how/index.php?page=3>.

"IrisPass." 2001-2002. OKI Global Site. 7 November 2003. <http://www.oki.com/jp/FSC/iris/en>.

"Jetstream." 1999-2002. EyeTicket Products. 8 November 2003. <http://www.eyeticket.com/en/index.php?section=products&body=jetstream>.

"LG Iris Recognition System – IrisAccess 3000." 2003. LG Electronics / Iris Technology Division. 7 November 2003. <http://www.lgiris.com>.

Mansfield, Tony, Gavin Kelly, David Chandler, and Jane Kane. CESG Contract X92A/4009309 Biometric Product Testing Final Report. Draft 0.6. Middlesex: National Physical Laboratory, 19 March 2001.

Meehan, Michael. "Iris scans take off at airports." July 2000. ComputerWorld. 7 November 2003. <http://www.computerworld.com/securitytopics/security/story/0,10801,47202,00.html>.

Mrozek, Werner. "IriScan – Biometrics for secure recognition." December 2000. Biometric News. 7 November 2003. <http://www.euro-security.de/en/html/iriscan_-_biometrics_for_secur.html>.

Penny, Wayne. "Biometrics: A Double Edged Sword – Security and Privacy". 2003. SANS Reading Room. 7 November 2003. <http://www.sans.org/rr/papers/index.php?id=137>.

"A Practical Guide to Biometric Security Technology". 2001 IT Professional: Technology Solutions for the Enterprise. 7 November 2003. <http://www.computer.org/itpro/homepage/jan_feb01/security3b.htm>.

"Product Showcase." 2003. Panasonic Ideas for Life.7 November 2003. <http://www.panasonic.com/cctv/showcase/>.

"Proof Positive: Certification Configuration." 2003. Iridian technologies: Proof Positive. 7 November 2003. <http://www.iridiantech.com/products.php?page=5&sub=a>.

"Selected Solutions: Selected Case Studies." 2003. Iridian Technologies. 19 November 2003. <http://www.iridiantech.com/solutions.php?page=2>.

Soto, Carlos A. "Biometrics gets better but still needs some work". Government Computer News 05/05/03; Vol 22 No. 10. 7 November 2003. <http://www.gcn.com/22_10/prod_reviews/21949-1.html>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced